УГОЛОВНО-ПРАВОВЫЕ НАУКИ
CRIMINAL LAW SCIENCES

CC BY

Оригинальное теоретическое исследование

УДК 343

https://doi.org/10.23947/2949-1843-2026-4-2-66-73

EDN: EEIYHW

Преступления в сфере компьютерной информации: уголовно-правовой аспект

А.Ж. Киселева ✉, **Р.В. Киселев**

Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

✉ kiseleva17@bk.ru

Аннотация

Введение. Преступления в сфере компьютерной информации являются наиболее динамично развивающейся уголовно-правовой категорией в условиях глобальной цифровизации. В Уголовном кодексе Российской Федерации существует отдельная глава, статьи которой устанавливают уголовную ответственность за преступные деяния, предметом посягательства которых выступает компьютерная информация. Актуальность данного исследования обусловлена возникающими проблемами в правоприменительной практике, различием научных позиций по квалификации анализируемых деяний и существующими пробелами уголовного законодательства РФ. Цель статьи – определение сущности компьютерных преступлений, анализ научных позиций и правоприменительной практики для выявления наиболее проблемных аспектов при квалификации преступлений в сфере компьютерной информации.

Материалы и методы. Основу исследования составили УК РФ, нормативные правовые акты, регламентирующие общественные отношения в сфере охраняемой законом информации, материалы судебной практики, научные труды. В ходе исследования использовались формально-юридический, системно-структурный и правоприменительный методы.

Результаты исследования. Выявлено, что существующие сложности в квалификации преступлений в сфере компьютерной информации обусловлены их латентностью, высокой технологичностью и трансграничным характером. Терминологическая неопределенность уголовно-правовых характеристик деяний, закрепленных в гл. 28 УК РФ, и бланкетные диспозиции отдельных статей определяют значительный круг проблем для правоприменителя при квалификации. Анализ показал, что, в условиях стремительно усложняющихся способов совершения преступлений с помощью технологий искусственного интеллекта и нейросетей, большинство ученых склоняются к необходимости уточнения предмета посягательств и расширения перечня объектов анализируемых преступлений. Принятие Постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 в значительной степени обеспечило единообразный подход к рассмотрению уголовных дел судами, однако в полном объеме имеющиеся проблемы не разрешены.

Обсуждение и заключение. Результаты исследования свидетельствуют о том, что проблемы квалификации неправомерного доступа к компьютерной информации и преступлений, связанных с использованием вредоносных программ, обусловлены сложностью технической природы рассматриваемых деяний и постоянным развитием способов их совершения, несовершенством отдельных уголовно-правовых конструкций, отсутствием единообразного толкования ряда признаков состава преступления. Решение указанных проблем требует совершенствования уголовного законодательства и судебной практики, повышения качества экспертного обеспечения расследования компьютерных преступлений.

Ключевые слова: компьютерные преступления, сфера компьютерной информации, квалификация преступлений, объект и субъект преступления, судебная практика, Уголовный кодекс Российской Федерации

Благодарности. Авторы выражают благодарность рецензентам, чья критическая оценка материалов и предложения по их совершенствованию способствовали значительному повышению качества статьи.

© Киселева А.Ж., Киселев Р.В., 2026

Для цитирования. Киселева А.Ж., Киселев Р.В. Преступления в сфере компьютерной информации: уголовно-правовой аспект. *Правовой порядок и правовые ценности.* 2026;4(2):66–73. https://doi.org/10.23947/2949-1843-2026-4-2-66-73

Original Theoretical Research

Cybercrimes: Criminal Law Perspective

Anna Zh. Kiseleva ✉, **Roman V. Kiselev**
Don State Technical University, Rostov-on-Don, Russian Federation
✉ kiseleva17@bk.ru

Abstract

Introduction. In the context of global digitalization, cybercrimes are considered to be the most rapidly developing category in the criminal law. The Criminal Code of the Russian Federation includes a separate chapter with the articles stipulating criminal liability for encroachments upon computer information. The relevance of the study is underpinned by the challenges encountered during law enforcement, as well as by the divergence of scientific attitudes towards the qualification of the criminal acts under study, and the existing gaps in the criminal law of the Russian Federation. The aim of the article is to define the essence of cybercrimes, to analyse the scientific attitudes and law enforcement practices in order to identify the most problematic aspects in qualifying the cybercrimes.

Materials and Methods. The research was based on the study of the Criminal Code of the Russian Federation, legal acts regulating social relations on handling the information protected by law, judicial practice materials, and scientific publications. The research was carried out using the dogmatic, system-structural and law enforcement methods.

Results. It has been revealed that the existing difficulties in qualifying the cybercrimes stem from their latent, highly technological, and cross-border nature. The terminological ambiguity of the criminal-law definitions of the acts enshrined in Chapter 28 of the Criminal Code of the Russian Federation and the blanket disposition of certain articles lead to a significant number of difficulties for a law-enforcer to qualify these acts. The analysis has revealed that, in the context of rapid sophistication of crimes committed using artificial intelligence and neural networks, the majority of scholars tend to believe in the need to specify the subject of the criminal encroachment and expand the list of objects susceptible for committing the crimes under study. The adoption of the Resolution No. 37 of the Plenum of the Supreme Court of the Russian Federation of December 15, 2022, has to great extent ensured a uniform approach of the courts to consideration of such criminal cases; however, the existing problems have not been fully resolved.

Discussion and Conclusion. The findings obtained during the research indicate that the difficulties in qualifying unlawful access to computer information and crimes involving the use of malware stem from the technical complexity of the crimes under study and constant evolution of the methods of committing thereof, the imperfection of certain legal constructs of criminal law, and the lack of a uniform interpretation of the certain signs of corpus delicti. For solving the revealed problems, it is required to improve the criminal law and judicial practices, as well as enhance the quality of expert support of cybercrime investigations.

Keywords: cybercrimes, the sphere of computer information, qualification of crimes, object and subject of a crime, judicial practices, the Criminal Code of the Russian Federation

Acknowledgements. The authors are grateful to the reviewers for critical evaluation of the materials and suggestions for their improvement that contributed to the significant enhancement of the quality of the article.

For Citation. Kiseleva AZh, Kiselev RV. Cybercrimes: Criminal Law Perspective. *Legal Order and Legal Values*. 2026;4(2):66–73. https://doi.org/10.23947/2949-1843-2026-4-2-66-73

Введение. Компьютерные преступления в условиях глобальной цифровизации представляют собой одну из наиболее динамично развивающихся категорий современной преступности вследствие широкого распространения автоматизированных электронных систем, нейросетей, различных устройств коммуникации. Анализ уголовной ответственности за компьютерные преступления в разных государствах свидетельствует о значительном разнообразии подходов к определению этого вида преступлений. Впервые закон об ответственности за компьютерные преступления был принят в США в 1984 г., впоследствии неоднократно изменялся и дополнялся, на данный момент включен в виде отдельного параграфа Титула 18 Свода законов США. Законом были установлены уголовные санкции не только за неправомерный доступ, но и за выход за пределы разрешенного доступа к защищенной ЭВМ. При этом защищенная ЭВМ одновременно выступает и в качестве предмета преступного

деяния. В указанных нормах определены 7 составов преступных деяний, обусловленных несанкционированным доступом посредством ЭВМ к защищенным правительственным базам и системам, сведениям о финансовой информации потребителей, повреждением или уничтожением информации о защищенной ЭВМ, мошенническими действиями, шантажом и угрозами, совершаемыми с помощью ЭВМ, и др.

Вслед за США нормативные правовые акты, устанавливающие уголовную ответственность за преступления данного вида, были приняты Германией (УК ФРГ 1987 г.) и Великобританией (Закон о злоупотреблениях компьютерами 1990 г. и Закон о терроризме 2000 г.). Указанные государства не вывели данный вид преступлений в отдельные составы, фактически общеуголовные преступления квалифицируются как компьютерные, если совершены с использованием ЭВМ или предметом преступного посягательства является информация, защищаемая государством и хранимая в базах данных, электронных системах и т. д.

В России законодатель пошел по иному пути, закрепив в УК РФ главу 28, регламентирующую уголовную ответственность за преступления в сфере компьютерной информации. Предметом указанных деяний выступает фактически любая компьютерная информация. Анализируемая глава расположена в разделе «Преступления против общественной безопасности и общественного порядка», т. е. законодателем подчеркивается значительная общественная опасность данных преступных посягательств [1].

Цель статьи – определение сущности компьютерных преступлений, анализ научных позиций и правоприменительной практики для выявления наиболее проблемных аспектов при квалификации преступлений в сфере компьютерной информации.

Материалы и методы. Эмпирическую базу исследования составили: Уголовный кодекс РФ, Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37, нормативные правовые акты, регламентирующие общественные отношения в сфере охраняемой законом информации, материалы судебной практики, научные публикации. Использовались формально-юридический, системно-структурный (анализ основных характеризующих признаков состава компьютерных преступлений) и правоприменительный (определение устойчивых позиций судов по вопросам квалификации преступления по нормам гл. 28 УК РФ) методы.

Результаты исследования. Предметом анализируемых посягательств выступает информация, имеющая электронную форму и хранящаяся (обрабатывающаяся) на специальных устройствах или с помощью специальных вычислительных мощностей (хостов, серверов, мобильных устройств, ЭВМ и т. д.). С учетом тех сведений, которые содержатся в «компьютерной» информации, она может подлежать охране посредством иных норм УК РФ. К примеру, если субъект совершил преступное деяние, посягающее на режим использования государственной тайны, повлекшее ее разглашение, и при этом способом совершения явились, например, неразрешенный доступ к электронных данным или используемая вредоносная компьютерная программа, то указанные действия будут квалифицированы по совокупности ст. 283 (разглашение государственной тайны) и ст. 272/273 УК РФ. В таком же режиме квалифицируются преступные деяния, связанные с неразрешенным воздействием с помощью ЭВМ на информацию и в других сферах жизнедеятельности [2]. Указанная позиция изложена и в Постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[1].

Тем не менее в научной доктрине не утихает дискуссия по этому вопросу: некоторые авторы, отчасти не соглашаясь с позицией Верховного Суда РФ, обосновывают точку зрения о том, что не все преступления, совершаемые с использованием ЭВМ, должны квалифицироваться по совокупности с нормами гл. 28 УК РФ [3]. Стоит отметить, что до принятия указанного постановления судебная практика характеризовалась значительной неоднородностью: одни и те же деяния судами различных регионов Российской Федерации квалифицировались неодинаково, что противоречит принципу законности и единообразия применения уголовного закона.

Уголовный кодекс РФ относит указанные преступные деяния к преступлениям, родовым объектом которых выступает общественный порядок и общественная безопасность, а видовым – компьютерная информация, которая законодателем понимается в самом широком смысле. Законодатель закрепляет, что такой информацией являются сведения в форме электрических сигналов[2]. Согласно методическим рекомендациям Генеральной прокуратуры РФ, указанные преступления посягают в первую очередь на общественные отношения, возникающие в связи с созданием, хранением, обработкой и использованием компьютерной информации. К примеру, если речь

[1] *О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».* Постановление Пленума Верховного Суда РФ № 37 от 15.12.2022. URL: https://www.vsrf.ru/documents/own/31913/?ysclid=mqqqxqjnpu558939244 (дата обращения: 15.04.2026).

[2] *Уголовный кодекс Российской Федерации.* Кодекс Российской Федерации № 63-ФЗ от 13.06.1996. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891&ysclid=mqqr05bnps440838494 (дата обращения: 15.04.2026).

идет о диспозиции ст. 272 УК РФ, то здесь объектом посягательства будут общественные отношения, складывающиеся по поводу неправомерного доступа, создания, хранения, модификации, использования компьютерной информации самим создателем и потребления ее иными пользователями[3].

При этом юридическая доктрина не выработала единого подхода к пониманию преступлений в сфере компьютерной информации. Одни авторы связывают преступные посягательства этого вида с воздействием не только на компьютерную информацию, но и на информационные технологии, используемые для реализации преступного умысла, которые в таком случае являются предметом преступления [4]. Другие авторы используют для обозначения преступлений этого вида очень разнообразные формулировки: «киберпреступления», «преступления, совершаемые с помощью информационно-телекоммуникационных технологий», «компьютерные преступления» и др. [5]. Отметим, что в статьях гл. 28 УК РФ помимо термина «компьютерная информация» употреблены такие понятия, как «цифровая» или «электронная» информация, «средства хранения, обработки и передачи информации», «данные», «информационно-телекоммуникационные сети» и т. п., однако их содержание либо имеет одинаковый смысл, либо не раскрыто в нормах. И.В. Семенова и И.Н. Кондрат подчеркивают, что нормы уголовного законодательства, устанавливающие ответственность за преступные деяния данного вида, обладают терминологической перегруженностью, а использование значительного числа одинаковых по смыслу понятий осложняет правоприменение и препятствует формированию единой позиции при квалификации преступлений [6].

Преступления анализируемой категории безусловно обладают признаком высокой технологичности, соответственно, преступные схемы совершенствуются гораздо интенсивнее, нежели уголовно-правовая охрана нарушаемых данными деяниями интересов, а также правоприменительная практика. В этой связи существует проблематика толкования отдельных понятий при выявлении признаков объективной стороны преступлений этого вида [7]. Некоторые авторы также отмечают, что законодательные термины, используемые для обозначения сути анализируемых преступлений, имеют в основном технический характер и в необходимом объеме не отражают сущности предмета охраны. В такой интерпретации упущено множество цифровых объектов информационной среды, которая состоит не только из сведений, представляющих собой электрические сигналы.

Определенные трудности в этом смысле также вызывает бланкетный характер норм анализируемых составов. К примеру, ст. 274.1 УК РФ апеллирует понятиями специального закона (Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»[4]), которые имеют специализированный характер, что значительно усложняет правоприменительную деятельность. Практикам при квалификации данного деяния необходимо владеть не только уголовно-правовыми категориями, но и пониманием терминов вышеназванного закона.

К.Н. Евдокимов указывает, что следователи и суды испытывают трудности в определении объектов и субъектов критической инфраструктуры, признаков неправомерного воздействия и характера угрозы [8]. Особенно остро данная проблема проявляется на современном этапе в виду стремительного развития цифровых платформ, технологий искусственного интеллекта и распределенных сетей. Фактически значительное число форм компьютерной преступности не могут быть определены используемой в УК РФ терминологией. В этой связи правоприменитель зачастую вынужден толковать действующие уголовно-правовые нормы расширительно, что обуславливает высокий риск нарушения одного из основных принципов уголовного права – законности.

М.И. Лавицкая и И.Н. Крапчатова полагают, что, несмотря на усилия законодателя по уточнению норм гл. 28 УК РФ, по-прежнему имеют место правореализационные проблемы, связанные с несовершенством уголовно-правовых предписаний. К примеру, в анализируемой главе УК РФ отсутствует легальная дефиниция «вредоносная программа» (ст. 273 УК РФ), при этом в диспозиции статьи используется термин «компьютерная программа», который не закреплен законодательно [9].

Более того, необходимо отметить трансграничный характер компьютерных преступлений: деяние может быть совершено в отношении защищаемой информации одного государства, при этом само деяние (в данном случае преступные действия) непосредственно совершалось на территории другого государства (к примеру, с помощью устройств для блокировки или несанкционированного доступа, расположенных в другом государстве) [10]. Такие примеры демонстрируют определенные сложности в организации расследования данных общественно опасных деяний, что обуславливает необходимость активного международного сотрудничества со стороны правоохранительных органов.

---

[3] *Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации*. Утв. Генпрокуратурой России 14.04.2014. URL: https://epp.genproc.gov.ru/ru/gprf/documents/4900250-e5958088/?ysclid=mqqr27m5qx637422433 (дата обращения: 13.04.2026).

[4] *О безопасности критической информационной инфраструктуры Российской Федерации*. Федеральный закон № 187-ФЗ от 26.07.2017. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102439340&intelsearch=%D4%E5%E4%E5%F0%E0%EB%FC%ED%FB%E9+%E7%E0%EA%EE%ED+%EE%F2+26.07.2017+%B9187-%D4%C7&ysclid=mqqr78735p374244992 (дата обращения: 15.04.2026).

Указанные преступления имеют достаточно сложную конструкцию объективной стороны, поскольку для правильной квалификации, помимо прочего, необходимо устанавливать способ доступа к информации и механизмы обхода систем защиты, вид последствий и характер воздействия на охраняемую информацию (модификация, блокировка, уничтожение, несанкционированное копирование и т. д.). В этой связи при расследовании указанных преступлений необходимо привлечение специалистов в области компьютерных технологий и обработки компьютерной информации, а также проведение соответствующих технических экспертиз.

Как отмечено в работе А.В. Безрукова и О.В. Безруковой [11], в нынешней действительности информация, генерируемая с помощью компьютерных технологий, сама по себе обладает экономической значимостью, поскольку неправомерный доступ к сведениям, содержащимся в ней, способен причинить значительный ущерб репутации, имуществу и т. п., а также является серьезной угрозой государственной безопасности. В этом смысле особую опасность представляют преступления, посягающие на критическую инфраструктуру нашего государства (объекты жизнеобеспечения, транспорта, энергетики, банковской системы и т. д.), поскольку общественно опасным последствием здесь выступает нарушение нормальной жизнедеятельности государства и общества в целом (остановка производства, аварии, отключение систем ЖКХ, причинение вреда здоровью и жизни населения, экологические катастрофы).

Немаловажной характеристикой компьютерных преступлений, осложняющей правильную и последовательную квалификацию деяний, является и то, что данные деяния зачатую выступают способом совершения других видов преступлений. Е.А. Русскевич отмечает, что в современных условиях неправомерный доступ к компьютерной информации становится универсальным способом совершения большого количества общественно опасных деяний [12]. Например, это может быть получение злоумышленниками доступа к мобильному банку потерпевшего путем использования фишинговых сайтов или поддельных SMS-сообщений в целях перевода денежных средств на подконтрольные счета. В таких ситуациях указанные действия должны быть квалифицированы по совокупности составов, например, по ст. 272 УК РФ и по п. «г» ч. 3 ст. 158 УК РФ.

Исходя из анализа судебной практики, деяния, образующие состав преступления, предусмотренного ст. 272 УК РФ, наиболее распространены и одновременно являются одной из наиболее сложных для квалификации форм посягательств на охраняемую законом информацию. Диспозиция указанной статьи отражает, что преступным является неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло блокирование, модификацию, уничтожение либо копирование компьютерной информации. Несмотря на простоту и логичность диспозиции, на практике возникают значительные сложности при выявлении объективных и субъективных характеристик преступления, так как достаточно сложно установить отличие между правомерным или неправомерным поведением. Наиболее остро эта проблематика проявляется, когда речь идет об использовании учетных записей, баз данных и корпоративных систем, либо же программ удаленного администрирования. В частности, работник может обладать правом доступа к информационной системе организации, но при этом использовать находящиеся в ней сведения за пределами своих полномочий. Фактически в данной ситуации возникают сомнения, считается ли такой доступ неправомерным.

Особое значение для правильной квалификации указанных деяний имеет постановление Пленума Верховного Суда РФ от 15.12.2022 № 37, в котором указано, что под неправомерным доступом следует понимать доступ, осуществляемый в отсутствие законных оснований или с нарушением порядка доступа к компьютерной информации. Таким образом, доступ будет считаться неправомерным при нарушении режима использования информации даже при наличии технического разрешения (логина и пароля, дающих соответствующий доступ), что в принципе соответствует изложенной выше позиции Верховного Суда РФ.

Законодатель также связывает наличие состава преступления, предусмотренного ст. 272 УК РФ, с наступлением общественно опасных последствий в виде блокирования, модификации, уничтожения или копирования в нашем случае именно компьютерной информации. Ранее судебная практика длительное время неоднозначно оценивала последствия, что приводило к различным подходам к квалификации одинаковых деяний. Сложности также вызывает установление факта модификации информации. Изменение отдельных технических параметров системы, автоматическое обновление файлов или изменение метаданных не всегда свидетельствуют о наличии признаков преступления. Для единообразного понимания наступающих в результате неправомерного доступа последствий в постановлении Пленума Верховного Суда РФ даны характеристики вышеуказанных понятий [13].

Отдельного внимания заслуживает проблема квалификации действий, связанных с использованием вредоносного программного обеспечения [14]. Нередко неправомерный доступ осуществляется посредством использования либо вирусов и различных фишинговых ресурсов, либо программ автоматизированного подбора паролей. В данной ситуации возникает вопрос о разграничении составов преступлений по ст. 272 и 273 УК РФ. Верховный

Суд РФ разъяснил, что в случае, если неправомерный доступ осуществлялся с использованием вредоносной программы, деяние подлежит квалификации по совокупности вышеуказанных составов преступлений.

Также на практике сложности вызывают дела, связанные с использованием программ удаленного администрирования. Подобное программное обеспечение само по себе является законным и широко применяется для технического обслуживания компьютерных систем. Однако использование таких программ без согласия владельца устройства может образовывать состав преступления, предусмотренного ст. 273 УК РФ. В подобных ситуациях правоприменителю необходимо устанавливать, имелась ли у виновного цель несанкционированного воздействия на компьютерную информацию либо на средства ее защиты.

В условиях повсеместного использования сети Интернет, в т. ч. для осуществления преступной деятельности, нормы гл. 28 УК РФ приобретают особенную значимость. Несмотря на то, что законодатель систематически совершенствует данную главу, последние принятые изменения и дополнения тем не менее не могут в полном объеме обеспечить уголовно-правовую охрану цифровых правоотношений. К примеру, если рассматривать состав преступления, предусмотренный ч. 1 ст. 274.2 УК РФ, то для правильного понимания его объективной стороны необходимо учитывать иные нормативные правовые акты, регламентирующие в т. ч. технические требования к установке и эксплуатации систем безопасности для надежного функционирования сети Интернет. При этом ответственность наступает при условии, что преступление совершено должностным лицом или индивидуальным предпринимателем (ИП), которые были ранее подвергнуты административной ответственности (ч. 2 ст. 13.42 КоАП РФ). Соответственно к субъектам данного преступления относятся ИП, которые могут быть, допустим, поставщиком интернет-услуг либо владельцем агрегатора компьютерной информации (различные онлайн-платформы для реализации товаров и оказания услуг).

Вопрос отнесения ИП к субъектам компьютерных преступлений широко обсуждается в научных кругах ввиду некоторых противоречий между гражданским, административным и уголовным законодательством. В частности, физическое лицо имеет возможность зарегистрироваться в качестве ИП с 14 лет (при наличии согласия законных представителей), при этом возраст уголовной ответственности за компьютерные преступления (в т. ч. по ч. 1 ст. 274.1 УК РФ), исходя из норм ст. 20 УК РФ, наступает с 16 лет. Административная ответственность, с учетом формулировки ч. 1 ст. 274.1 УК РФ, также наступает с 16 лет. При этом на основании ч. 2 ст. 2.3 КоАП РФ решением комиссии по делам несовершеннолетних лицо в возрасте от 16 до 18 лет может быть освобождено от ответственности с применением к нему иных мер воздействия. Таким образом, теоретически возникает ситуация, при которой несовершеннолетний, совершивший правонарушение по ч. 2 ст. 13.42 КоАП РФ, а впоследствии и уголовно-наказуемое деяние, предусмотренное, к примеру, ч. 1 ст. 274.1 УК РФ, не будет подлежать ответственности в принципе.

С учетом вышеизложенного, на наш взгляд, целесообразно внести корректировки в КоАП РФ и УК РФ, снизив возраст ответственности до 14 лет для лиц, осуществляющих предпринимательскую деятельность или работающих по трудовому договору (ст. 2.3 КоАП РФ), а также для лиц, совершивших преступление по ст. 274.1 УК РФ (ст. 20 УК РФ).

Обсуждение и заключение. Полученные результаты подтверждают, что преступления в сфере компьютерной информации представляют собой сложную и многоаспектную категорию общественно опасных деяний, которая отличается латентностью, технологичностью [15], трансграничностью и постоянным эволюционированием. Современная судебная практика характеризуется постепенным формированием единых подходов к квалификации данных деяний, чему немало поспособствовало принятие Постановления Пленума Верховного Суда РФ от 15.12.2022 № 37. Однако законодательство РФ по-прежнему имеет некоторые пробелы и требует корректировки в части определения возраста уголовной ответственности за совершение компьютерных преступлений, установления объективных признаков, квалификации неправомерного доступа к компьютерной информации и преступлений, связанных с использованием вредоносных программ, и некоторых других аспектов. Решение указанных проблем требует совершенствования уголовного законодательства, развития судебной практики, повышения качества экспертного обеспечения расследования компьютерных преступлений и подготовки специалистов в сфере цифровой криминалистики.

Список литературы / References

1. Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше). *Вестник Томского государственного педагогического университета.* 2006;11(62):30–35.

Gromov EV. Development of Criminal Legislation on Cybercrimes in Foreign Countries (USA, Great Britain, Germany, the Netherlands, Poland). *Tomsk State Pedagogical University Bulletin*. 2006;11(62):30–35. (In Russ.)

2. Щепельков В.Ф. О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ). *Уголовное право.* 2023;6(154):70–79.

Shchepelkov VF. On the Qualification of Cybercrimes (in Light of the Clarifications of the Plenum of the Supreme Court of the Russian Federation). *Criminal Law*. 2023;6(154):70–79. (In Russ.)

3. Карчевская Н.И., Семенова И.В. Интеграция преступных деяний, квалифицированных по главе 28 УК РФ, в экстремистскую деятельность. *Мировой судья.* 2025;(12):23–27.

Karchevskaya NI, Semenova IV. Integration of Criminal Acts under Chapter 28 of the Criminal Code of the Russian Federation into Extremist Activities. *Magistrate Judge*. 2025;(12):23-27. (In Russ.)

4. Дворецкий М.Ю., Копырюлин А.Н. *Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации*. Тамбов: Тамбовский государственный университет им. Г.Р. Державина; 2006. 212 с.

Dvoretsky MYu, Kopyryulin AN. *Optimization of Criminal Liability and Problems of Qualification of Crimes in the Sphere of Computer Information*. Tambov: Tambov State University named after G.R. Derzhavin; 2006. 212 p. (In Russ.)

5. Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие. *Правовой порядок и правовые ценности.* 2023;1(1):126–136. https://doi.org/10.23947/2949-1843-2023-1-1-126-136

Vitvitskaya SS, Vitvitsky AA, Isakova YuI. Cybercrimes: Concept, Classification, International Countering. *Legal Order and Legal Values*. 2023;1(1):126-136. (In Russ.) https://doi.org/10.23947/2949-1843-2023-1-1-126-136

6. Семенова И.В., Кондрат И.Н. К вопросу о терминологической перегрузке норм Уголовного кодекса Российской Федерации в контексте преступлений, связанных с цифровой информацией. *Мировой судья.* 2025;(11):8–12.

Semenova IV, Kondrat IN. On Terminological Overload of Provisions of the Criminal Code of the Russian Federation within the Framework of Crimes Related to Digital Information. *Magistrate Judge*. 2025;(11):8–12. (In Russ.)

7. Лысак Е.А. Проблемы квалификации преступлений в сфере компьютерной информации. *Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета.* 2013;(90):997–1006.

Lysak EA. Problems of Qualification of Computer Crimes. *Polythematic Online Scientific Journal of Kuban State Agrarian University (Scientific Journal of KubSAU).* 2013;(90):997–1006. (In Russ.)

8. Евдокимов К.Н. К вопросу совершенствования квалификации преступлений в сфере компьютерной информации. *Российский судья.* 2025;(2):36–40. https://doi.org/10.18572/1812-3791-2025-2-36-40

Evdokimov KN. On Improving the Qualification of Crimes in the Field of Computer Information (Based on Judicial Practice). *Russian Judge.* 2025;(2):36–40. (In Russ.) https://doi.org/10.18572/1812-3791-2025-2-36-40

9. Лавицкая М.И., Крапчатова И.Н. Структурно-содержательная характеристика главы 28 УК РФ: юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации. *Российский следователь.* 2021;(6):35–41.

Lavitskaya MI, Krapchatova IN. The Structural and Content Characteristics of Chapter 28 of the Criminal Code of the Russian Federation: Legal Writing and Law Enforcement Problems of Constituent Elements of Crimes Involving Computer Information. *Russian Investigator.* 2021;(6):35–41. (In Russ.)

10. Кузина С.И., Сагирян И.Г. Кибертерроризм как реальная угроза национальной безопасности Российской Федерации. *Правовой порядок и правовые ценности.* 2023;1(4):46–57. https://doi.org/10.23947/2949-1843-2023-1-4-46-57

Kuzina SI, Sagiryan IG. Cyberterrorism as a Real Threat to the National Security of the Russian Federation. *Legal Order and Legal Values*. 2023;1(4):46–57. (In Russ.) https://doi.org/10.23947/2949-1843-2023-1-4-46-57

11. Безруков А.В., Безрукова О.В. Преступления в сфере компьютерной информации: юридический анализ, проблемы квалификации. *Эпомен.* 2020;(42):28–39.

Bezrukov AV. Bezrukova OV. Crimes in the Field of Computer Information: Legal Analysis, Problems of Qualification. *Epomen*. 2020;(42):28–39. (In Russ.)

12. Русскевич Е.А. О совокупности преступлений в сфере компьютерной информации с другими преступлениями. *Уголовное право.* 2025;(4(176)):76–84. https://doi.org/10.52390/20715870_2025_4_76

Russkevich EA. On Conjunction of Crimes in the Sphere of Computer Information with Other Crimes. *Criminal Law*. 2025;(4(176)):76–84. (In Russ.) https://doi.org/10.52390/20715870_2025_4_76

13. Нафиков М.М. Проблемы квалификации преступлений в сфере компьютерной информации. В: *Труды II Всероссийской научно-практической конференции «Уголовная политика в условиях цифровой трансформации» (Казань, 27 апреля 2023 г.).* Казань: Издательство «Отечество»; 2023. С. 117–123.

Nafikov MM. Problems of Qualification of Crimes in the Field of Computer Information. In: *Proceedings of the II All-Russian Scientific and Practical Conference "Criminal Policy in the Context of Digital Transformation". Kazan, April 27, 2023.* Kazan: Otechestvo Publishing House; 2023. P. 117–123. (In Russ.)

14. Хатов Э.Б. Киберпреступление. *Законность.* 2026;(3(1097)):46–49.

Khatov EB. Cybercrime. *Zakonnost* (*Legality)*. 2026;(3(1097)):46–49. (In Russ.)

15. Харламова А.А., Щетинина Н.В. Преступление, предусмотренное ч. 2 ст. 274.2 УК РФ: комментарий новеллы. *Уголовное право.* 2025;(10(182)):60–66. https://doi.org/10.52390/20715870_2025_10_60

Kharlamova AA, Shchetinina NV. The Crime under Part 2 of Art. 274.2 of the Criminal Code of the Russian Federation: Commentary on the Innovation. *Criminal Law*. 2025;(10(182)):60–66. (In Russ.) https://doi.org/10.52390/20715870_2025_10_60

Об авторах:

Анна Жунусовна Киселева, кандидат юридических наук, доцент кафедры «Гражданское право» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), SPIN-код, ORCID, ScopusID, kiseleva17@bk.ru

Роман Валерьевич Киселев, старший преподаватель кафедры «Уголовное право и публично-правовые дисциплины» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), ORCID, krv1980@mail.ru

Заявленный вклад авторов:

А.Ж. Киселева: формирование основной концепции, цели и задач исследования, подготовка текста, формирование выводов.

Р.В. Киселев: анализ правоприменительной практики, формирование выводов и предложений, доработка текста.

Конфликт интересов: **авторы заявляют об отсутствии конфликта интересов.**

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Anna Zh. Kiseleva, Cand.Sci. (Law), Associate Professor of the Civil Law Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), SPIN-code, ORCID, ScopusID, kiseleva17@bk.ru

Roman V. Kiselev, Senior Lecturer of the Criminal Law and Public Law Disciplines Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), ORCID, krv1980@mail.ru

Claimed Contributorship:

AZh Kiseleva: formulating the main concept, aim and objectives of the research, preparing the text, formulating the conclusions.

RV Kiselev: analysis of law enforcement practices, formulating the conclusions and proposals, refining the text.

Conflict of Interest Statement: **the authors declare no conflict of interest.**

The authors have read and approved the final manuscript.

Поступила в редакцию / Received 06.05.2026
Поступила после рецензирования / Reviewed 25.05.2026
Принята к публикации / Accepted 01.06.2026